
Interns Ian Stewart (white shirt), Tegan Durtschi (grey shirt) and Jordan Todd (not pictured), thwarted a mock cyberheist to win their division in a Department of Defense Cyber Challenge.

# INL interns win high-school division in national cyber challenge

by Sara Prentice, *INL Communications & Governmental Affairs*

Idaho National Laboratory cybersecurity researcher Bryan Hatton saw potential in the young men digging through trash and scouting thrift stores for parts to build computers. So he recruited them as interns and encouraged them to compete in the national Digital Forensics Challenge. His instincts paid off.

Ian Stewart, Tegan Durtschi and Jordan Todd — summer interns for the Department of Homeland Security's Control System Security Program at INL — thwarted a mock cyberheist, won first place in their division and a trip to the Department of Defense's Cyber Conference in St. Louis. Attendees remarked on the trio's skills, assuming the interns cracked the case using a store-bought product rather than their own ingenuity.


***The Department of Defense and the SANS (SysAdmin, Audit, Network, Security) Institute sponsor the annual DC3: Digital Forensics Challenge.***

"I didn't have any expectations going in," Durtschi said. "We were surprised how well we placed."

The DC3: Digital Forensics Challenge competition is sponsored by the Department of Defense and the SANS (SysAdmin, Audit, Network, Security) Institute. Now in its fourth year, the event simulates challenges an actual digital forensic investigator might face in the lab.

As soon as Stewart, Durtschi and Todd arrived at INL to begin their internships, Hatton encouraged them to compete. The team agreed, but members said they never expected to win.

"I guess my primary motivation was the free trip to St. Louis," Durtschi said.

But their first order of business was to name their team. The interns chose "pwnage," hacker jargon pronounced "P-ownage", which means to compromise or control, specifically another computer, Web site, gateway device or application.

Team Pwnage then got to work. The interns were given two DVDs containing images of a hard drive and a case file. The case file explained the mock scenario: police were suspicious a suspect might be planning a warehouse heist. It was up to Stewart, Durtschi and Todd to collect evidence that could prevent the heist. They were to look for things like pictures of items to be stolen, guns and conversations with possible accomplices.

Password cracking was just one of the new tools and programs they had to learn and employ along the way. Python, a programming language, helped them accomplish the challenges associated with cracking the hard drive.

***Stewart (left) and Durtschi accepted their awards at the Department of Defense's Cyber Conference in St. Louis.***

Parsing the log files created by Skype allowed them to find evidence that the suspect had used an Internet instant messaging program to plan the heist. Once the team was able to decode the binary code, it could read conversations the suspect had with accomplices.

They also worked with steganography, a method for hiding one type of data in another without it being detected. The team found several images on the hard drive that contained "steg" images, which helped them mount a case against the suspect.

Throughout the challenge, the team wrote more than 30 computer programs to help it clean up the hard drive and uncover information. If they got stuck on a particular problem, Hatton, their mentor, would nudge them in the right direction.

"It was cool; we learned everything from scratch," Stewart said. "The self-guided aspect, figuring it out on our own through research, was cool."

Team Pwnage took first place in the 58-team high school division and placed in the top 50 among undergraduate, graduate, military and non-U.S. teams.

In late January, Durtschi and Stewart flew to St. Louis to accept their award at the Department of Defense's Cyber Crime Conference.

The attendees of the conference were impressed with the students' skills. A "Hactor Factor" blogger called the group "sharp." And one winner from a different division asked what off-the-shelf forensic tool kit the team had used to unlock the hard drive. Hatton said the students didn't use any off-the-shelf products — they built their own kit using what they learned during their internships.

"The internship was cool because we got paid to learn," Durtschi said.

Feature Archive